



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/849,318	05/19/2004	Paul Gassoway	063170.7177	5789
5073 7590 02/22/2008 BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980				
EXAMINER LOUTE, OSCAR A				
ART UNIT		PAPER NUMBER		
2136				
NOTIFICATION DATE		DELIVERY MODE		
02/22/2008		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary

Application No.

10/849,318

Applicant(s)

GASSOWAY, PAUL

Examiner

OSCAR A. LOUIE

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-946)
- 3) ☐ Information Disclosure Statement(s) (PTO/SE/US)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

This final action is in response to the amendment filed on 11/20/2007. The examiner notes that the intention of his Examiner's Note regarding 35 U.S.C. 112 6th paragraph in the first office action on the merits was to address the possibility of there being an issue of structure in the applicant's disclosure in support of their Claims. That is, there appeared to be no issues seen by the examiner upon the first correspondence to the applicant. The examiner has withdrawn his previous Examiner's Note to avoid confusion on behalf of the applicant. In light of the applicant's amendments, the examiner hereby withdraws his previous Claims rejections regarding Claims 5, 11, & 17. Claims 1-24 are pending and have been considered as follows.

Claim Objections

1. Claim 19 is objected to because of the following informalities:
 - Claim 19 lines 1 & 2 recite, "for" and "being operable to" which should be "...configured to..."

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1).

Claims 1, 7, 13, & 19:

Vaidya discloses a method, system, and computer recording medium including computer executable code for maintaining security of a computer system comprising,

- “determining an initial system certainty value for the computer system” (i.e. “attack signature profiles to the data collectors 10 based on the network configuration”) [column 5 lines 31-33];
- “providing access to a database of signatures” (i.e. “the data repository 12 includes a database handler 26 which polls the data collectors 10 for intrusion detection data and stores the data for future reference”) [column 5 lines 47-50];
- “each signature including a signature certainty value” (i.e. “The attack signature profile type can be either simple, sequential or a timer/counter based”) [column 7 lines 2-4];
- “receiving data” (i.e. “The remote network 24 is connected to the LAN 11 and is equipped with a data collector 10 which monitors work stations located on the remote

network 24 and transmits network security data specific to the remote network back to the data repository 12. Both the remote network 24 and the LAN 11 are connected to the global communications network referred to as the Internet”) [column 5 lines 39-46];

- “comparing the received data with the database of signatures” (i.e. “The attack signature profiles are adapted for detecting network data patterns associated with network intrusions which include unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction in a network object”) [column 5 lines 33-39];
- “filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data” (i.e. “If in step 64 the data collector 10 determines that the data packet is not associated with a network intrusion, the data collector continues to monitor data in step 58. If a network intrusion is detected, the reaction module is notified in step 66. The reaction module 38 takes steps to trace the application session associated with the data packet, to terminate the session, and/or to notify the network administrator”) [column 7 lines 4-11];

but Vaidya does not explicitly disclose,

- “increasing the system certainty value if the received data does not match a signature in the database”
- “decreasing the system certainty value if the received data matches a signature in the database”

however, Vaidya does disclose,

- “A timer/counter based attack signature profile directs the virtual processor 36 to execute instructions associated with a single expression on every data packet associated with a particular application session to determine whether an event has occurred a threshold number of times within a predetermined time interval” [column 8 lines 16-21];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, “increasing the system certainty value if the received data does not match a signature in the database” and “decreasing the system certainty value if the received data matches a signature in the database,” in the invention as disclosed by Vaidya for the purposes of determining whether a particular event has occurred a threshold number of times.

Claims 2, 8, 14, & 20:

Vaidya discloses a method, system, and computer recording medium including computer executable code for maintaining security of a computer system, as in Claims 1, 7, 13, & 19 above respectively, but do not explicitly disclose,

- “the data that does not match a signature in the database is forwarded to its destination”

however, Vaidya does disclose,

- “indicating which network objects are not permitted to access other network objects”

[column 6 lines 34-35];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the data that does not match a signature in the database is forwarded to its destination," in the invention as disclosed by Vaidya since the recitation of network objects not being permitted access to other network objects would imply that under any other condition, network objects would be permitted access.

Claims 4, 10, 16, & 22:

Vaidya discloses a method, system, and computer recording medium including computer executable code for maintaining security of a computer system, as in Claims 1, 7, 13, & 19 above respectively, further comprising,

- "the data comprises a packet of data" (i.e. "data packets") [column 5 line 38].

Claims 5, 11, 17, & 23:

Vaidya discloses a method, system, and computer recording medium including computer executable code for maintaining security of a computer system, as in Claims 1, 7, 13, & 19 above respectively, but do not explicitly disclose,

- "the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value"
- "the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value"

however, Vaidya does disclose,

- "indicating which network objects are not permitted to access other network objects" [column 6 lines 34-35];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value" and "the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value," in the invention as disclosed by Vaidya since the recitation of network objects not being permitted access to other network objects would also imply that under any other condition, network objects would be permitted access. In addition, the invention disclosed by Vaidya includes determining malicious data packets based on signature thresholds which would be understood as permitting access if under one set of conditions (i.e. signature certainty value less than) and refusing access under all other conditions (i.e. signature certainty value greater than).

4. Claims 3, 6, 9, 11, 15, 18, 21, & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Moran (US-7032114-B1).

Claims 3, 9, 15, & 21:

Vaidya discloses a method, system, and computer recording medium including computer executable code for maintaining security of a computer system, as in Claims 1, 7, 13, & 19 above respectively, but do not disclose,

- "the increased or decreased certainty value becomes the initial system value"

however, Moran does disclose,

- "the high false positive rate typical of the real-time systems is reduced by filtering out false alerts using a broader range of information than the IDS can retain, and by allowing

the alert threshold to be set higher, because the inventive system can recover information about a suspicious session that occurred before the threshold was crossed” [column 8 lines 39-44];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “the increased or decreased certainty value becomes the initial system value,” in the invention as disclosed by Vaidya for the purposes of readjusting the threshold to reduce the possibility of a false positive under conditions which are applicable.

Claims 6, 12, 18, & 24:

Vaidya discloses a method, system, and computer recording medium including computer executable code for maintaining security of a computer system, as in Claims 5, 11, 17, & 23 above respectively, but do not disclose,

- “the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded”

however, Moran does disclose,

- “an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events, and assign a suspicion value to a record associated with an event” [column 4 lines 28-33];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded,” in the invention as disclosed by Vaidya for the purposes of recording timed information for future further analysis.

Response to Arguments

5. Applicant's arguments filed 11/20/2007 have been fully considered but they are not persuasive.

Arguments Regarding Vaidya:

- The applicant's arguments that Vaidya does not disclose, "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database" and "filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data," have been considered but are non-persuasive. Vaidya suggests the usage of a threshold that determines an event based on a certain frequency of matched results. It is suggested that the threshold may be set/selected accordingly, which provides suggestion to it being adjustable (i.e. increased/decreased). Vaidya also suggests that action would be taken upon a detection of an intrusion (i.e. a match is made based on the threshold) which provides suggestion that data is filtered based on the matching of intrusion detection signatures.

Argument Regarding the Combination of Vaidya and Moran:

- The applicant's argument that Moran, "fails to overcome this deficiency," has been considered but is non-persuasive. Moran suggests the adjustment of a threshold for an IDS.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private

Art Unit: 2136

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
02/15/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136